WHAT IS CLAIMED IS:

1. (Currently Amended) A signal processing apparatus for performing modular multiplication for use in a signal processing system, the apparatus comprising:

a first logic for outputting a signed multiplicand by selectively performing a one's complementary operation on a multiplicand according to a Booth conversion result of a multiplier in modular multiplication;

a second logic for outputting a modulus which is signed in the modular multiplication based on a carry input value Carry-in of a current clock, determined from a carry value cin for correction of a previous clock, and on a sign bit of the multiplicand; and

a third logic for receiving the signed multiplicand and the signed modulus, and calculating a result value of the modular multiplication by iteratively performing a full addition operation on a carry value C and a sum value S of the full addition operation, found at the previous clock.

2. (Cancelled)

3. (Currently Amended) The apparatus of claim 1, wherein the first logic receives two least significant bits of the multiplier and a predetermined reference bit while sequentially shifting bits of the multiplier, and performs the Booth conversion thereon.

4. (Cancelled)

5. (Cancelled)

6. (Currently Amended) The apparatus of claim 3, wherein the first logic comprises:

a Booth conversion circuit for performing the Booth conversion using the two least significant bits of the multiplier and the reference bit;

a multiplexer for multiplexing the multiplicand based on the two least significant bits of the multiplier; and

a one's complementer for outputting the signed multiplicand by selectively performing the one's complementary operation on the output of the multiplexer based on a sign bit of the Booth conversion result.

7. (Currently Amended) The apparatus of claim 1, wherein the third logic performs the full addition operation using at least two Carry Save Adders (CSAs) each including a plurality of full adders.

8. (Cancelled)

9. (Cancelled)

10. (Cancelled)

11. (Cancelled)

12. (Currently Amended) The apparatus of claim 1, wherein the third logic performs the full addition operation using at least two Carry Save Adders (CSAs) each including a plurality of full adders.

13. (Cancelled)

14. (Currently Amended) The apparatus of claim 1, wherein the second logic comprises:

a quotient logic for determining at every clock first bit values which are extracted by as many values as a predetermined number of bits, beginning from a least significant bit for each of the

carry value and the sum value calculated in the third logic, and second bit values for determining a multiple of modular reduction in the modular multiplication based on the carry input value Carry-in and a sign bit of the multiplicand; and

a selector for selecting the signed modulus based on the second bit values.

15. (Currently Amended) The apparatus of claim 1, wherein the third logic further comprises a full adder for outputting the carry input value Carry-in by performing the full addition operation using the carry value cin for correction and the sign bit of the multiplicand, received from the second logic.

16. (Currently Amended) The apparatus of claim 1, wherein the third logic performs a carry propagation addition operation on the carry value and the sum value output from the third logic after (m+2) clocks, where m=n/2, when each of the multiplier, the multiplicand and the modulus has n bits.

17. (Cancelled)

18. (Cancelled)

19. (Cancelled)

20. (Cancelled)

21. (Cancelled)

22. (Cancelled)

23. (Cancelled)

24. (Cancelled)

25. (Cancelled)

26. (Cancelled)

27. (Cancelled)

28. (Cancelled)

29. (Cancelled)

30. (Cancelled)

31. (Cancelled)

32. (Currently Amended) The apparatus of claim 15, wherein the third logic adds the modulus to the carry propagation addition operation result when a result of the carry propagation addition operation is a negative number.

A signal processing method for performing modular multiplication for use in a signal processing system, the method comprising:

outputting a signed multiplicand by selectively performing a one's complementary operation on a multiplicand according to a Booth conversion result of a multiplier in modular multiplication;

finding a carry input value Carry-in of a current clock determined from a carry value cin for

correction of a previous clock;

outputting a modulus which is signed in the modular multiplication based on the carry input value and a sign bit of the multiplicand; and

receiving the signed multiplicand and the signed modulus, and calculating a result value of the modular multiplication by iteratively performing a full addition operation on a carry value C and a sum value S of the full addition operation, found at the previous clock.

33. (Currently Amended) The method of claim 32, wherein outputting a signed multiplicand comprises:

receiving two least significant bits of the multiplier and a predetermined reference bit while sequentially shifting bits of the multiplier, and performing the Booth conversion thereon.

34. (Currently Amended) The method of claim 33, wherein the outputting of a signed multiplicand comprises:

performing the Booth conversion using the two least significant bits of the multiplier and the reference bit;

multiplexing the multiplicand based on the two least significant bits of the multiplier; and

outputting the signed multiplicand by selectively performing the one's complementary operation on the output of the multiplexed multiplicand based on a sign bit of the Booth conversion result.

35. (Cancelled)

36. (Cancelled)

37. (Cancelled)

38. (Cancelled)

39. (Cancelled)

40. (Cancelled)

41. (Cancelled)

42. (Currently Amended) The method of claim 33, wherein finding of a carry input value Carry-in comprises:

outputting the carry input value Carry-in by performing a full addition operation using the carry value cin for correction and the sign bit of the multiplicand.

43. (Cancelled)

44. (Cancelled)

45. (Cancelled)

46. (Currently Amended) The method of claim 32, further comprising performing a carry propagation addition operation on the carry value and the sum value after (m+2) clocks, where m=n/2, when each of the multiplier, the multiplicand and the modulus has n bits.

47. (Currently Amended) The method of claim 46, further comprising adding the modulus to the carry propagation addition operation result, when a result of the carry propagation addition operation is a negative value.

48. (Cancelled)

49. (Cancelled)

50. (Cancelled)

51. (Cancelled)

52. (Cancelled)

53. (Cancelled)

54. (Cancelled)

55. (Cancelled)

56. (Cancelled)

57. (Cancelled)

58. (Cancelled)

59. (Cancelled)

60. (Cancelled)

61. (Cancelled)

62. (Cancelled)

63. (Cancelled)

64. (New) The apparatus of claim 6, wherein the first logic outputs the signed multiplicand by selectively performing the one's complementary operation on the output of the multiplexed multiplicand based on a sign bit of the Booth conversion result.

65. (New) The method of claim 32, wherein the full addition operation is performed using at least two Carry Save Adders (CSAs) each including a plurality of full adders.

66. (New) The method of claim 32, wherein the outputting a signed modulus comprises:

extracting, at every clock, as many first bit values as a predetermined number of bits beginning from a least significant bit for each of the carry value and the sum value;

outputting second bit values for determining a multiple of modular reduction in the modular multiplication based on the first bit values, the carry input value Carry-in and a sign bit of the multiplicand; and

selecting the signed modulus based on the second bit values.

67. (New) The method of claim 32, wherein the outputting a signed multiplicand comprises:

outputting the signed multiplicand by selectively performing the one's complementary operation on the output of the multiplexed multiplicand based on a sign bit of the Booth conversion result.